JOURNAL OF ALGEBRA 91, 499–519 (1984)

Large Cyclic Subgroups of Finite Groups*

R. DVORNICICH AND M. FORTI

Dipartimento di Matematica, Università di Pisa, 56100 Pisa, Italy

Communicated by B. Huppert

Received May 19, 1983

INTRODUCTION

It follows from a theorem of Frobenius that for any divisor d of the order of a finite group G the number of solutions in G of the equation $x^d = 1$ is always a multiple of d (see [4, p. 44]).

It is well known that this number is always d iff the group is cyclic. Recently Hausmann and Shapiro [3] showed that if $|\{x \in G \mid x^d = 1\}| < \gamma d$ for any $d \mid |G|$, then there is a cyclic subgroup of G whose index is bounded by a function $I(\gamma)$ of γ alone.

In this paper the authors consider the size of the function $I(\gamma)$, giving explicit upper and lower bounds in the general case. The exact values of $I(\gamma)$ have been determined only for $\gamma \leqslant 10$ and are listed below:

γ	1	2	3	4	5	6	7	8	9	10
$I(\gamma)$	1	2	4	4	6	8	9	12	12	12

(see [1, 3]).

If special classes of groups are considered, much more can be said about the relations between the index of the largest cyclic subgroup and the number of the dth roots of 1. The authors do not deal with this subject here, and refer to [1, 2] for some results in this direction.

1. DEFINITIONS AND MAIN RESULTS

All the groups considered will be finite and the notation will usually be the standard one. In addition, if not otherwise stated explicitly, we shall denote

$$|G| = q_0^{a_0} \cdot \ldots \cdot q_h^{a_h} \quad \text{and} \quad \exp G = q_0^{a_0 - e_0} \cdot \ldots \cdot q_h^{a_h - e_h} \quad (q_0 < q_1 < \cdots < q_h)$$

the prime factorization of the order (resp. the exponent) of G.

* Research partially supported by G.N.S.A.G.A. of C.N.R.

0021-8693/84 $3.00

G_q any q-Sylow subgroup of G (and usually $|G_q| = q^a$, $\exp G_q = q^{a-e}$).
$\mathbf{N}_G(H)$, $\mathbf{C}_G(H)$ the *normalizer* (resp. the *centralizer*) in G of a subgroup H.
$\mathbf{Z}(G)$ the *center* of G.

$$\eta_G = \frac{|G|}{\exp G}$$

and

$$\mu_G = \frac{|G|}{\varphi(|G|)} \qquad \left(\varphi \text{ the Euler's function } \varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)\right)$$

$\iota_G = \min\{[G: \langle x\rangle] \mid x \in G\}$ the *cocyclicity* of G.
$\gamma_G(d) = 1/d|\{x \in G \mid x^d = 1\}|$.
$\gamma_G = \max\{\gamma_G(d) \mid d \mid |G|\}$ the *multiplicity* of G.
$I(\gamma) = \sup\{\iota_G \mid \gamma_G \leqslant \gamma\}$.
$I_h(\gamma) = \sup\{\iota_G \mid \gamma_G \leqslant \gamma$ and $|G|$ has $\leqslant h+1$ prime factors$\}$.
G is called *paracyclic* iff $\iota_G \leqslant \gamma_G$.
A *complement* of a subgroup H of G is a subgroup K verifying $HK = G$, $H \cap K = \{1\}$.
G is *q-nilpotent* iff G_q has an invariant complement.
The subscript G will usually be omitted when no ambiguity can arise.
The main results we shall prove about the size of the function $I(\gamma)$ are summarized in the following theorems.

THEOREM 1. *For any $\gamma > 2$ both*

$$I(\gamma) < \gamma^2 \tag{1.1}$$

and

$$I(\gamma) < \gamma^{1+(C_1/\log\log\gamma)} \tag{1.2}$$

hold.

Hence $I(\gamma) \ll \gamma^{1+\varepsilon}$. On the other hand $I(\gamma)/\gamma$ is unbounded:

THEOREM 2. *There exists an increasing sequence such that*

$$I(\gamma_n) > C_2 \gamma_n (\log\log \gamma_n)^{1/2}. \tag{1.3}$$

When the number of prime factors is fixed, more can be said, namely

THEOREM 3.

$$I_h(\gamma) < C^{(h)} \gamma \log^h \gamma. \tag{1.4}$$

The constants C_1, C_2, $C^{(h)}$ are absolute and explicitly determined; moreover $C^{(h)}$ tends rapidly to zero as h increases.

We shall need in the paper estimates for some arithmetical functions.

Since their proofs involve standard techniques and classical results, we refer to [5] and we simply list the inequalities we shall use.

We denote with $p_0 = 2, p_1, \ldots, p_n, \ldots$ the primes in their natural ordering (we shall use this notation throughout the paper). Then

$$n \log n < p_{n-1} < n(\log n + \log\log n) \qquad \text{(the last for } n \geqslant 6) \tag{1.A}$$

$$\sum_{i=1}^{n} \operatorname{loglog} p_i > \begin{cases} n \log(n+1) & \text{(for any } n) \\ (n+1)\log(n+1) & \text{(for } n > 37) \end{cases} \tag{1.B}$$

$$\begin{gathered} \sum_{i=1}^{n} \log p_i > \begin{cases} n \log(n+1) & \text{(for any } n) \\ (n+1)\log(n+1) & \text{(for } n \geqslant 16) \end{cases} \\ \sum_{i=1}^{n} \log p_i < (n+1)(\log(n+1) + \operatorname{loglog}(n+1)) \end{gathered} \tag{1.C}$$

$$\frac{m}{\varphi(m)} < e^C \operatorname{loglog} m + \frac{5}{2 \operatorname{loglog} m} \qquad \text{(for } 3 < m \neq 223092870) \tag{1.D}$$

where $C = 0.57721566\ldots$ is the Euler's constant

$$\prod_{i=0}^{n-1} \left(1 - \frac{1}{p_i}\right)^{-1} > e^C (\log n + \operatorname{loglog} n). \tag{1.E}$$

Remark that (1.B) and (1.C) are not included in [5], but are easily stated using the results and the techniques of [5]; (1.E) is a mere rephrasing of the corresponding estimate of [5].

2. General estimates for $I(\gamma)$

We start with a uniform estimate obtained by quantifying the method used in [3].

LEMMA 2.1. *The inequality*

$$\iota_G < \gamma_G \eta_G \mu_G \tag{2.1}$$

holds in any group G.

Proof. Define inductively the subgroups H_i, C_i of G by

$$H_0 = G,$$

$$C_0 = \text{a cyclic subgroup of } H_0 \text{ with largest } q_0\text{-power order,}$$

$$\text{say } q_0^{b_0} (= q_0^{a_0 - e_0}),$$

$$H_{i+1} = H_i \cap \mathbf{N}_G(C_i),$$

$$C_{i+1} = \text{a cyclic subgroup of } H_{i+1} \text{ with largest } q_{i+1}\text{-power order,}$$

$$\text{say } q_{i+1}^{b_{i+1}}.$$

Put

$$n_i = [H_i : H_{i+1}], \qquad m_i = \exp H_i / \exp H_{i+1}, \qquad l_i = n_i / m_i$$

$$n = n_0 \cdot \ldots \cdot n_h, \qquad m = m_0 \cdot \ldots \cdot m_h.$$

Note that, by construction, $C = C_0 C_1 \cdots C_h$ is a cyclic subgroup of $H = H_{h+1}$ and that $m = q_0^{a_0 - e_0 - b_0} \cdot \ldots \cdot q_h^{a_h - e_h - b_h}$.

Therefore $[G: C] = m\eta_G$.

Since C has exactly n conjugates, we get, by counting their generators,

$$n\varphi(|C|) + |C| - \varphi(|C|) \leqslant \gamma_G \cdot |C|. \tag{2.2}$$

The thesis now follows by remarking that $|C|/\varphi(|C|) \mid \mu_G$ and $m \mid n$.

Q.E.D.

Remark that (2.2) holds for any cyclic subgroup with at least n conjugates, hence also for the subgroup of C whose order is $\prod_{n_i \neq 1} q_i^{b_i}$.

Similarly

$$m < \gamma \prod_{m_i \neq 1} \frac{q_i}{l_i(q_i - 1)}.$$

Apparently the product on the right-hand side attains its maximum when all the l_i's are 1 and the occurring primes are most possible and the smallest ones.

Since, by construction, $q_j \mid m_i$ implies $j > i$, we may assume

$$p_1 \cdots p_k < \gamma \frac{p_0 \cdots p_{k-1}}{(p_0 - 1) \cdots (p_{k-1} - 1)}$$

where p_0, $p_1, \ldots, p_k, \ldots$ is the sequence of the prime numbers and $k = |\{i \mid m_i \neq 1\}|$.

Now an upper bound for m can be obtained by evaluating the function $v(\gamma)$ defined by

$$v(\gamma) = \max \left\{ \frac{n}{\varphi(n)} \;\middle|\; n = p_0 \cdots p_{k-1} < \gamma \frac{2n}{p_k \varphi(n)} \right\}$$

Noting that for $\gamma \neq 29$ the above condition implies $\gamma \geqslant n$, the estimate (1.D) gives

$$v(\gamma) < e^C \operatorname{loglog} \gamma + \frac{5}{2 \operatorname{loglog} \gamma}$$

for any $\gamma \neq 29$ and 223092870, and both these values can be tested directly.

Now the inequality (2.1) can be strengthened to

COROLLARY 2.2. *Put* $\gamma = \gamma_G$, $\eta = \eta_G$ *and* $v = v_G = \min(\mu_G, v(\gamma))$.

Then

$$\iota_G < \eta\gamma v. \tag{2.3}$$

In particular, for $\gamma \geqslant 3$

$$I(\gamma) < \gamma^2 \left(e^C \operatorname{loglog} \gamma + \frac{5}{2 \operatorname{loglog} \gamma} \right) \tag{2.4}$$

where C is the Euler's constant.

We shall use the notation $v_G = \min(\mu_G, v(\gamma_G))$ throughout the rest of the section.

More precise results can be obtained when the number of prime factors of G is bounded. To this aim, we introduce the following definition:

A set $\mathscr{D}$ of divisors of $|G|$ is *weakly dominating* for G iff $\forall\, g \in G\ \exists\, d \in \mathscr{D}$ such that $g^d = 1$.

$\mathscr{D}$ is *strongly dominating* (or simply *dominating*) if it is weakly dominating and its maximum is the order of some element of G.

The interest of dominating sets lies in the following

LEMMA 2.3. *Let* $\mathscr{D}$ *be weakly dominating for G, and put* $D = \sum_{d \in D} d$. *Then*

$$|G| \leqslant \gamma_G \cdot D. \tag{2.5}$$

If $\mathscr{D}$ *is dominating, then*

$$\iota_G \leqslant \gamma_G \frac{D}{\max \mathscr{D}} \leqslant \gamma_G \cdot |\mathscr{D}|. \tag{2.6}$$

The proof is immediate from the definitions. Let us remark that equality can hold only if $|\mathscr{D}| = 1$, and that (2.6) can be improved to $\iota_G \leqslant \gamma_G \cdot |\mathscr{D}|\,(1 - |\mathscr{D}| - 1)/2 \max \mathscr{D})$, for the elements of $\mathscr{D}$ are integers. However, if closer approximations are needed, it is more convenient to look directly at (2.5).

Note that from Lemma 2.3 it follows at once that any nilpotent group is paracyclic.

Put

$$\mathscr{D}(K; q_0,..., q_h) = \{n \in \mathbf{N} \mid K \leqslant n = q_0^{s_0} \cdot \ldots \cdot q_h^{s_h} < q_j K \quad \text{if } s_j > 0\}$$

$$D(K; q_0,..., q_h) = \sum_{d \in \mathscr{D}(K; q_0,\ldots,q_h)} \frac{1}{d}$$

$$t(K; q_0,..., q_h) = |\mathscr{D}(K; q_0,..., q_h)|$$

(shortly $\mathscr{D}(K, h)$, $D(K, h)$, $t(K, h)$ when $q_0,..., q_h$ are the first $h + 1$ primes).

Suppose the orders of the elements of G are bounded by M. Then the set $\{m = \exp G/d \mid d \in \mathscr{D}(\exp G/M; q_0,..., q_h)\}$ (where $q_0,..., q_h$ are the primes dividing $|G|$) is weakly dominating for G.

From Lemma 2.3 it follows immediately:

COROLLARY 2.4. *If* $\iota_G \geqslant K\eta_G$, *then*

$$\eta_G \leqslant \gamma_G D(K; q_0,..., q_h) \leqslant \gamma_G \frac{t(K; q_0,..., q_h)}{K}. \tag{2.7}$$

In particular

$$\iota_G \leqslant \gamma_G t(K; q_0,..., q_h) \tag{2.8}$$

whenever $K \geqslant \iota_G/\eta_G$.

Remark that the equality can hold in (2.7), (2.8) only in the trivial case $\iota_G = \eta_G$.

We need some estimates for the number of the integral points included in a symplex of given sides.

LEMMA 2.5. *Put*

$$\mathscr{S}(A_1,..., A_h) = \left\{x \in \mathbf{N}^h \;\middle|\; \sum_{i=1}^{h} x_i/A_i < 1\right\}$$

and

$$\mathscr{E}(A_0,..., A_h) = \left\{x \in \mathbf{N}^{h+1} \mid 1 \leqslant \sum_{i=0}^{h} x_i/A_i < 1 + \frac{1}{A_j} \text{ if } x_j \neq 0\right\}.$$

For $I \subseteq \{1,..., h\}$ *put*

$$A(I) = \prod_{i \in I} A_i \qquad \text{and} \qquad \sigma(I) = \sum_{i \in I} \frac{1}{A_i}.$$

Then

$$|\mathscr{S}(A_1,\ldots,A_h)| < \sum_{\sigma(I)<1} \frac{A(I)}{I!}$$

and

$$|\mathscr{E}(A_0,\ldots,A_h)| < \sum_{\sigma(I)<1} \frac{A(I)}{I!} |\{j \mid I \subseteq \{j+1,\ldots,h\}\}|.$$

Assume $A_0 \geqslant A_1 \geqslant \cdots \geqslant A_h$ *and either* $\sigma(1,\ldots,k+1) \geqslant 1$ *or* $k = h$. *Then*

$$|\mathscr{S}(A_1,\ldots,A_h)| < A_1 \cdot \ldots \cdot A_k \sum_{s=0}^{k} \frac{\binom{h}{s}}{s!} \left(\frac{\sigma(1,\ldots,k)}{k}\right)^{k-s}$$

$$|\mathscr{E}(A_0,\ldots,A_h)| < A_1 \cdot \ldots \cdot A_k \sum_{s=0}^{k} \frac{\binom{h+1}{s+1}}{s!} \left(\frac{\sigma(1,\ldots,k)}{k}\right)^{k-s}. \tag{2.9}$$

Proof. First of all remark that the map $(x_0,\ldots,x_h) \mapsto (x_{j+1},\ldots,x_h)$, where $j = \min\{i \mid x_{i+1} \neq 0\}$ gives a 1–1 correspondence between $\mathscr{E}(A_0,\ldots,A_h)$ and the disjoint union of the symplexes $\mathscr{S}(A_{j+1},\ldots,A_h)$. Hence all estimates for $|\mathscr{E}|$ follow from the corresponding ones for $|\mathscr{S}|$.

Let $\mathscr{S}^0(A_1,\ldots,A_h) = \{x \in \mathscr{S} \mid x_i > 0 \ \forall i\}$. Clearly any point $x \in \mathscr{S}^0$ is included with the whole hypercube $\{z \in \mathbf{R}^h \mid x_i - 1 \leqslant z_i < x_i\}$ in the symplex of $\mathbf{R}^h$ with the same sides of $\mathscr{S}$.

Hence $|\mathscr{S}^0|$ is bounded by the volume $A_1 \cdot \ldots \cdot A_h/h!$ of the symplex. To be more accurate we could take into account that the polycube cannot cover the whole symplex (if $h > 1$); actually the covered region has volume $\leqslant (1 - 1/A_1)A_1 \cdot \ldots \cdot A_h/h!$.

Since the points with some coordinate zero belong to a symplex of lower dimension and since not all the x_i's with $i \in I$ can be strictly positive if $\sigma(I) \geqslant 1$, the first two inaqualities of the lemma are proved.

Now, given the further assumptions, only monomials of degree $\leqslant k$ can appear in the sums (2.9). Since their mean value cannot exceed the mean value of the terms of degree s in $(A_1 + \cdots + A_k)^s$, namely $A_1 \cdot \ldots \cdot A_k(\sigma(1,\ldots,k)/k)^{k-s}$, the inequalities (2.9) are proved. Q.E.D.

The estimate we shall use are summarized in the following:

COROLLARY 2.6. *Assume* $A_0 \geqslant A_1 \geqslant \cdots \geqslant A_h$ *and either* $k = h$ *or* $1/A_1 + \cdots + 1/A_{k+1} \geqslant 1$.

Then the following inequalities hold:

$$|\mathscr{S}(A_1,\ldots,A_h)| < \binom{h}{k}\frac{A_1\cdot\ldots\cdot A_k}{k!}\min\{(1+\sigma)^k,(1+\tau+\cdots+\tau^k)\}$$
$$|\mathscr{E}(A_0,\ldots,A_k)| < \binom{h+1}{k+1}\frac{A_1\cdot\cdots\cdot A_k}{k!} \tag{2.10}$$
$$\times\min\left\{(1+\sigma)^{k+1},(1+\tau+\cdots+\tau^k)+\frac{\tau}{k}\right\}$$

where $\sigma = 1/A_1+\cdots+1/A_k$ *and* $\tau = \sigma k/(h-k+1)$.

Proof. We have

$$\frac{k!}{\binom{h}{k}}\sum_{s=0}^{k}\frac{\binom{h}{s}}{s!}\left(\frac{\sigma}{k}\right)^{k-s} \leqslant \sum_{s=0}^{k}\binom{k}{s}\frac{k(k-1)\cdots(s+1)}{k^{k-s}}\sigma^{k-s} \leqslant (1+\sigma)^k$$

together with

$$\frac{k!}{\binom{h}{k}}\sum_{s=0}^{k}\frac{\binom{h}{s}}{s!} = \sum_{s=0}^{k}\frac{(k(k-1)\cdots(s+1))^2}{(h-s)\cdots(h-k+1)}\left(\frac{\sigma}{k}\right)^{k-s}$$
$$\leqslant \sum_{s=0}^{k}\left(\frac{\sigma k}{h-k+1}\right)^{k-s}.$$

Hence the first of the inequalities (2.10) follows from (2.9). Similarly one gets

$$\frac{k!}{\binom{h+1}{k+1}}\sum_{s=0}^{k}\frac{\binom{h+1}{s+1}}{s!}\left(\frac{\sigma}{k}\right)^{k-s} \leqslant (1+\sigma)^{k+1}$$

and, for $s \neq k-1$,

$$\frac{k!}{\binom{h+1}{k+1}}\frac{\binom{h+1}{s+1}}{s!}\left(\frac{\sigma}{k}\right)^{k-s} \leqslant \left(\frac{\sigma k}{h-k+1}\right)^{k-s}.$$

For $s = k-1$ the summand is $\sigma(k+1)/(h-k+1)$, and the extra-term τ/k provides the difference.

By considering the correction terms for the volumes of the polycubes (see the proof of the preceding lemma), one can neglect τ/k in many cases (e.g., if $k \leqslant (h+1)/2$ or $\sigma \geqslant 1 - 1/(k+1)$). Q.E.D.

Clearly

$$t(K; q_0, \ldots, q_h) = \left| \mathscr{E}\left(\frac{\log K}{\log q_0}, \ldots, \frac{\log K}{\log q_h}\right) \right|.$$

The basic result about groups having orders with $h+1$ prime factors can now be obtained by combining (2.10) with (2.8), namely:

THEOREM 2.7. *Put* $|G| = q_0^{a_0} \cdots q^{a_h}$, $\gamma = \gamma_G$ *and* $Q = (\log q_1) \cdots (\log q_h)$. *Then*

$$\iota_G < \frac{1+\varepsilon}{Q \cdot h!} \gamma (\log \gamma)^h$$

where $\varepsilon = \varepsilon_h(\gamma)$ *tends to zero as* γ *increases.*

More generally, for $\gamma > \Gamma_h = \varphi(p_0 \cdot \ldots \cdot p_h)$

$$I_h(\gamma) < C^{(h)} \gamma (\log \gamma)^h$$

where

$$C^{(h)} = \frac{5}{h!} \left(\frac{2}{\log(h+1)}\right)^h.$$

Proof. We apply (2.8) with $K = \gamma \mu_G$, as Lemma 2.1 allows.

The first inequality follows directly from Corollary 2.6 (with $k = h$).

To get a bound independent of the primes of $|G|$, we assume that $q_0, \ldots, q_h$ are the smallest primes.

Assuming $\gamma \geqslant \varphi(p_0 \cdots p_h)$, we get

$$\sigma = \frac{\sum \log p_i}{\log \mu_G \gamma} \leqslant 1.$$

Then

$$I_h(\gamma) < \gamma \log^h \gamma \frac{(1+\sigma)^{h+1}}{h! \log^h(h+1)} \left(1 + \frac{\log \mu_G}{\log \gamma}\right)^h$$

for $\log p_1 \cdot \ldots \cdot \log p_h > \log^h(h+1)$ by (1.B).

To get the desired bound for $C^{(h)}$, it suffices to show that

$h \log \mu_G \leqslant d \log \gamma$ with $d = \log 5/2$. This follows by induction on h starting from $h = 5$. A direct computation gives the result for $h < 5$. Q.E.D.

Thus Theorem 3 is proved.

We remark that any other choice of the lower bound Γ_h for γ would slightly affect the involved constant $C^{(h)}$. We have chosen this particular value since we conjecture that for smaller values of γ only fewer primes are essentially involved.

When h is very small, the estimate of Theorem 2.7 can be easily improved by considering which kind of numbers can occur in a dominating set of divisors, and evaluating directly $D(K; q_0 \cdots q_h)$ (see [2] for some examples).

We can obtain a uniform estimate for $I(\gamma)$ by the techniques of Theorem 2.7 if we may reduce ourselves to consider groups G where the number of prime factors of $|G|$ is bounded by a function of γ_G.

It is easily seen that if G_q is in the center of G, then

$$\gamma_{G/G_q} = \gamma_G/\gamma_{G_q} \qquad \text{and} \qquad \iota_{G/G_q} = \iota_G/\iota_{G_q};$$

hence the primes whose Sylow subgroups are in the center of G can be neglected.

Less trivial restrictions are given by the following lemmas.

LEMMA 2.8. *Suppose $G = NH$ with N cyclic and normal in G and $(|N|, |H|) = 1$. Let $\mathscr{D}$ be a dominating set for H and put $D = \sum_{d \in \mathscr{D}} d$. Then*

$$\iota_G \leqslant \gamma_G \frac{D}{\max \mathscr{D}} \leqslant \gamma_G |\mathscr{D}|.$$

In particular if $\iota_H \leqslant R\eta_H$, then

$$\iota_G \leqslant \gamma_G \cdot t(R; q_{i_0}, \ldots, q_{i_k})$$

where $q_{i_0}, \ldots, q_{i_k}$ are the prime factors of H.

Proof. Let $\mathbf{C}(N) = N \times K$, $A = H/K$, $\exp A = d$.

We have $\iota_G \leqslant \iota_H \cdot d$, since $x^d \in \mathbf{C}(N)$ for any $x \in H$. Let $E = \{x \in G \mid (o(x), |N|) = 1\}$. By our assumptions we obtain

$$|E| \leqslant \gamma_G \cdot D \leqslant \gamma_G \cdot \frac{|H|}{\eta_G \cdot R} t(R; q_{i_0}, \ldots, q_{i_k}).$$

To get the thesis it suffices to prove that $|E| \geqslant d|H|$.

Let $A = \prod_{q \mid |A|} A_q \cong \prod_q \prod_{j=1}^{l_q} \mathbf{Z}/(q^{\delta_j^{(q)}})$ be a direct decomposition of A verifying $\delta_j^{(q)} \geqslant \delta_{j'}^{(q)}$ if $j \geqslant j'$.

For any q choose an element $x_q \in A_q$ of order $q^{\delta_1^{(q)}}$, a Sylow subgroup

$N_{p(q)}$ of N such that the automorphism induced by x_q has order $q^{\delta_1^{(q)}}$, and a complement B_q of $\langle x_q \rangle$ in A_q inducing the identity on $N_{p(q)}$.

Pick a representative $x \in H$ of $\prod x_q$, let B be the subgroup of H including K corresponding to $\prod B_q$ and put $M = \prod N_{p(q)}$.

Remark that given $b \in B$ and $m \in M$, the element $x^i bm$ belongs to E iff for any $p \mid o(m)$ x^i is outside the centralizer of M_p.

Hence we have

$$|E| \geqslant |B| \sum_{s \mid d} \varphi(s) \prod_{x^{d/s} \notin \mathbf{C}(N_{p(q)})} |N_{p(q)}|$$

and $|E| \geqslant d\,|H|$ if the above sum is at least d^2.

Finally the inequality $\sum_{s \mid d} \varphi(d/s) \prod_{x^s \notin \mathbf{C}(N_{p(q)})} |N_{p(q)}| \geqslant d^2$ can be easily checked if there is a unique N_p for any q.

If more than one N_p occurs, the inequality follows by considering that $p-1$ is always even, whence there is at least an extra-factor 2 for any $s = q \neq 2$. Q.E.D.

Recalling that any normal Sylow subgroup G_q has a complement in G, we can apply the above lemma taking N as the product of all cyclic normal Sylow subgroups of G.

COROLLARY 2.9. *The inequalities* (2.7) *and* (2.8), *as well as the statements of Theorem* 2.7 *continue to hold for any group* G *if we restrict* $q_0, \ldots, q_h$ *to the primes whose Sylow subgroups are not simultaneously cyclic and normal.*

Lemma 2.8 has another interesting consequence which we already stated in [2] by a different proof.

Recall that a group G is said paracyclic if $\iota_G \leqslant \gamma_G$; then

COROLLARY 2.10. *If all the Sylow subgroups of* G *are cyclic* (*i.e.* , *if* $\eta_G = 1$), *then* G *is paracyclic.*

Proof. By a theorem of Zassenhaus (see [4, IV.2.11]), G is the semidirect product of two cyclic subgroups of relatively prime orders.

Call N (resp. H) the normal (resp. non-normal) one: the proof of Lemma 2.8 gives at once $\iota_G \leqslant \iota_H \cdot d = d$, $|H|\,\gamma_G \geqslant |E| \geqslant d\,|H|$. Q.E.D.

Also the cyclic Sylow subgroups lying in the center of their normalizers can be essentially neglected in the estimates of Theorem 2.7. In fact:

LEMMA 2.11. *Suppose* $G = NC$ *with* N *normal in* G, C *cyclic and* $(|N|, |C|) = 1$.

Put $\mathbf{N}(C) = H \times C$. Let $\mathscr{D}$ *be a dominating set for* H *and put* $D = \sum_{d \in \mathscr{D}} d$. *Then*

$$\iota_G < \mu_C \gamma_G \frac{D}{\max \mathscr{D}} \leqslant \mu_C \gamma_G |\mathscr{D}|.$$

In particular, if $\iota_H \geqslant R\eta_H$, *then*

$$\iota_G < \mu_C \gamma_G t(R; q_{i_0}, \ldots, q_{i_k})$$

where $q_{i_0}, \ldots, q_{i_k}$ *are the prime factors of* $|H|$.

Proof. By counting the elements of order multiple of $|C|$ we obtain

$$\varphi(|C|) \cdot |N| < \gamma_G \sum_{d \in \mathscr{D}} |C|\, d$$

where $\mathscr{D}$ is any dominating set of exponents for H. The first inequality now follows, since $\iota_G \leqslant \iota_H \cdot [N: H]$. By choosing, as usual,

$$\mathscr{D} = \left\{ d \;\middle|\; \exp H \mid d \leqslant \frac{\exp H}{R} < dq_l \text{ if } dq_l \;\middle|\; \exp H \right\}$$

we get the second inequality, and the lemma is proved. Q.E.D.

We recall that, by a theorem of Burnside [4, IV.2.6], any Sylow subgroup lying in the center of its normalizer has an invariant complement in G. Hence from Lemma 2.11 we can deduce:

COROLLARY 2.12. *If* $q_0, \ldots, q_h$ *are the primes whose Sylow subgroups are not simultaneously cyclic and in the center of their normalizer, then the inequalities* (2.7) *and* (2.8) *as well as the statements of Theorem* 2.7 *hold if the right-hand sides are multiplied by*

$$v_G = \min(\mu_G, v(\gamma)).$$

LEMMA 2.13. *Let* $G_{q_1}, \ldots, G_{q_l}$ *be cyclic Sylow subgroups of* G. *Assume that there exists a cyclic subgroup* C *with* $C = q_1^{\alpha_1} \cdots q_l^{\alpha_l}$ *and that no subgroup* C_i *of* C *with* $|C_i| = q_i^{\alpha_i}$ *is normal in* G. *Then* C *has at least* $q_1 \cdot \ldots \cdot q_l + 1$ *conjugates in* G.

Proof. We put $n_i = [G: \mathbf{N}(C_i)]$ and we use induction on l.
If $l = 1$, then

$$n_1 = \frac{[G: \mathbf{N}(G_{q_1})]}{[\mathbf{N}(C_1): \mathbf{N}(G_{q_1})]} \equiv 1(q_1).$$

Moreover if $n_1 = n_2 = \cdots = n_l$ the congruence $n_i \equiv 1(q_i)$ gives the result.

Assume $n_1 \geqslant n_2 \geqslant \cdots \geqslant n_s > n_{s+1} = n_{s+2} = \cdots = n_l$, hence $n_l \geqslant q_{s+1} \cdot \ldots \cdot q_l + 1$. By the induction hypothesis, $[G: \mathbf{N}(C_1 \cdot \ldots \cdot C_s)] \geqslant q_1 \cdot \ldots \cdot q_s + 1$. If for any $i > s$ $\mathbf{N}(C_i) \not\supseteq \mathbf{N}(C_1 \cdot \ldots \cdot C_s)$, then $\mathbf{N}(C_1 \cdot \ldots \cdot C_l)$ has index $\geqslant q_{s+1} \cdot \ldots \cdot q_l + 1$ in $\mathbf{N}(C_1 \cdot \ldots \cdot C_s)$ (again by induction). If there exists $i > s$ such that $\mathbf{N}(C_i) \supseteq \mathbf{N}(C_1 \cdot \ldots \cdot C_s)$, then $\mathbf{N}(C_i)$ is not included in any of the $\mathbf{N}(C_j)$'s $(j \leqslant s)$, for $n_j > n_i$.

Then $[\mathbf{N}(C_i): \mathbf{N}(C_1 \cdot \ldots \cdot C_s)] \geqslant q_1 \cdot \ldots \cdot q_s + 1$ by the induction hypothesis, and the lemma follows. Q.E.D.

COROLLARY 2.14. *Let* $\mathscr{Q} = \{q \mid G_q$ *is cyclic and not normal*$\}$. *Then*

$$\sum_{q \in \mathscr{Q}} \log q < 2 \log \gamma_G \nu_G.$$

Proof. Let C be the cyclic subgroup of G constructed in the proof of Lemma 2.1, and let $\mathscr{Q}_1 = \{q \in \mathscr{Q} \mid q \mid [G: C]\}$. Then Lemma 2.1 gives

$$\sum_{q \in \mathscr{Q}_1} \log q < \log \nu\gamma$$

whereas Lemma 2.13 gives

$$\sum_{q \in \mathscr{Q} - \mathscr{Q}_1} \log q < \log \nu\gamma \qquad \text{Q.E.D.}$$

Since $q \mid \eta_G$ if G_q is not cyclic, we have $q_0 \cdot \ldots \cdot q_h < \gamma_G^2 \eta_G \nu_G^2$ whenever no Sylow subgroup of G is simultaneously cyclic and normal.

In particular, when dealing with inequalities of the type (2.7), (2.8), it may be assumed w.l.o.g. that

$$(h+1)^{h+1} < \tfrac{1}{2}\nu^2\gamma^2\eta.$$

It is now possible to formulate the second half of Theorem 1 in the following way:

THEOREM 2.15. *If* $\gamma > 2$, *then*

$$I(\gamma) <_\gamma 1 + \frac{1 + \log 27/4}{\operatorname{loglog} \gamma - \operatorname{logloglog} \gamma - 1}.$$

Proof. Note that the above bound is worse than (2.4) if $\gamma < 10^{70}$, say; we may therefore assume γ large if necessary.

Moreover we may assume that the $h+1$ prime factors of $|G|$ are the

smallest ones and that $\sum_{i=1}^{h} \log p_i = \lambda \log v\gamma$ with $\lambda < 3$ by the above remark.

Let k verify $\sum_{i=1}^{k} \log p_i < \log v\gamma \leqslant \sum_{i=1}^{k+1} \log p_i$ (put $k = h$ if $\lambda < 1$).

Then (2.8) and (2.10) give

$$\iota_G < \gamma \frac{\binom{h+1}{k+1}}{k!} \left(\frac{\log v\gamma}{\log(k+1)}\right)^k \min\left\{(1+\sigma)^{k+1}, (1+\tau+\cdots+\tau^k)+\frac{\tau}{k}\right\} \tag{2.11}$$

with

$$\sigma = \frac{\sum_1^k \log p_i}{\log v\gamma} \qquad \text{and} \qquad \tau = \frac{\sigma k}{h-k+1}.$$

Since if $\lambda \geqslant 1$ then $\lambda/h > 1/(k+1)$, it is easy to see that $\binom{h+1}{k+1} \min\{(1+\sigma)^{k+1}, (1+\tau+\cdots+\tau^k)+\tau/k\} < 2\binom{3k+3}{k+1}$ when $0 < \lambda < 3$.

Then (2.11) yields

$$\iota_G < \gamma \binom{3k+3}{k+1} \exp \frac{\log v\gamma}{\log(k+1)}. \tag{2.12}$$

Recalling the definition of k, (1.C) gives

$$(k+1)\log(k+1) < \log v\gamma, \text{ since } \gamma \text{ is large enough.}$$

The right-hand side of (2.12) being increasing with k, we may take $\log v\gamma/\log(k+1) = k+1$, obtaining

$$\iota_G < \gamma \left(\frac{27}{4}\right)^{k+1} e^{k+1} < \gamma(v\gamma)^{(1+\log 27/4)/\log(k+1)}.$$

Now $v \leqslant v(\gamma) < e^c \operatorname{loglog} \gamma + 5/2e^c \operatorname{loglog} \gamma$ by (1.D). Substituting the value $\log(k+1) = \operatorname{loglog} v\gamma - \operatorname{loglog}(k+1)$, it is straightforward to check that

$$\log(k+1) > (\operatorname{loglog} \gamma - \operatorname{logloglog} \gamma - 1) \cdot \left(\frac{\log v}{\log \gamma} + 1\right).$$

Thus Theorem 2.15 is proved. Q.E.D.

From the above theorem it is easy to get an explicit value for the constant C_1 of Theorem 1 (for instance one may take $C_1 = 6$).

To get the first part of Theorem 1, we must consider $KD(K, h)$ instead of $|\mathscr{D}(K, h)|$. We begin with some simple sufficient conditions.

LEMMA 2.16. *In order that* $\iota_G < \gamma_G^2$, *either of the following conditions suffices*:

(i) *either* $\eta \leqslant \gamma/v$ *or* $\eta \geqslant \gamma D(\gamma, h)$;

(ii) *there exists* $K \leqslant \gamma/D(\gamma, h)$ *such that* $D(K, h) \leqslant 1/v$.

In particular $\iota < \gamma^2$ if $D(\gamma, h) \leqslant 1/v$.

Proof. Since $\iota < \eta\gamma v$, the first part of (i) suffices.

Recall that $\mathscr{D}(K, h)$ is weakly dominating iff $\iota/\eta \geqslant K$, and that in this case $\eta < \gamma D(k, h)$. Then the second part of (i) implies $\iota/\eta < \gamma$.

In particular if $D(\gamma, h) \leqslant 1/v$ the condition (i) is always true, whence the last assertion of the lemma.

Now assume $1/v < \eta/\gamma < D(\gamma, h) = D_0$ (otherwise (i) holds) and pick K verifying the condition (ii). If $\iota/\eta > K$ then $\eta < \gamma D(K, h) \leqslant \gamma/v$, against our hypothesis.

If $\iota \leqslant K\eta$ then $\iota < \gamma/D_0 \cdot \gamma D_0 = \gamma^2$. Q.E.D.

An upper bound for $D(K, h)$ is given by the following:

LEMMA 2.17. *For any non-negative* $\lambda < 1$ *and for any* $K \geqslant 1$

$$D(K, h) < K^{-\lambda} \prod_{i=1}^{h} \left(1 - \frac{1}{p_i^{1-\lambda}}\right)^{-1}. \tag{2.13}$$

Proof. Pick $d = p_0^{s_0} \cdots p_h^{s_h} \in \mathscr{D}(K, h)$. Then $K^\lambda \leqslant p_0^{\lambda s_0} \cdots p_h^{\lambda s_h}$ whence

$$\frac{1}{d} \leqslant K^{-\lambda} \left(\frac{1}{p_0^{1-\lambda}}\right)^{s_0} \cdots \left(\frac{1}{p_h^{1-\lambda}}\right)^{s_h} \leqslant K^{-\lambda} \frac{1}{(p_1^{1-\lambda})^{s_1} \cdots (p_h^{1-\lambda})^{s_h}}.$$

Although the 2-power factor has been deleted, the h-tuples $(s_1, \ldots, s_h)$ remain different from each other by the definition of $\mathscr{D}(K, h)$.

Hence

$$D(K, h) < K^{-\lambda} \sum_{s_1 \cdots s_h = 0}^{\infty} \frac{1}{p_1^{s_1(1-\lambda)} \cdots p_h^{s_h(1-\lambda)}} = K^{-\lambda} \prod_{i=1}^{h} \left(1 - \frac{1}{p_i^{1-\lambda}}\right)^{-1}.$$

Q.E.D.

COROLLARY 2.18. *Suppose that* $|G|$ *has at most* $h + 1$ *prime factors. Then* $\iota_G < \gamma_G^2$ *if*

$$\gamma_G^{\lambda(1+\lambda)} \geqslant v_G \prod_{i=1}^{h} \left(1 - \frac{1}{p_i^{1-\lambda}}\right)^{-1-\lambda}. \tag{2.14}$$

Proof. Since $D(K, h)$ is increasing in h for any K, we may freely apply the inequality (2.13).

The condition (ii) of Lemma 2.16 yields $\iota < \gamma^2$ provided

$$(\gamma/D(\gamma, h))^{-\lambda} \prod_{i=1}^{h} \left(1 - \frac{1}{p_i^{1-\lambda}}\right)^{-1} \leqslant \frac{1}{\gamma}.$$

Estimating $D(\gamma, h)$ again by (2.13) we get (2.14). Q.E.D.

By means of the standard techniques one gets immediately for $D(K, h)$ an estimate of the kind

$$D(K, h) \leqslant K^{-\lambda} \exp\left(\sum_{i=1}^{h} \frac{1}{p_i^{1-\lambda}} + A \cdot \sum_{i=1}^{h} \frac{1}{p_i^{2-2\lambda}}\right)$$

where A is a suitable constant depending only on λ.

We are interested in the case $\lambda = \frac{1}{2}$ and we shall deal only with it. In this case we have (see also [5])

$$\prod_{i=1}^{h} \left(1 - \frac{1}{\sqrt{p_i}}\right)^{-1} < \exp\left(a \left(\frac{h+1}{\log(h+1)}\right)^{1/2} + b \operatorname{loglog}(h+1) + c\right) = g(h).$$

For $h \geqslant 16$ the involved constants can be taken as follows:

$$a = 1.57 \qquad b = 0.57 \qquad c = 0.31.$$

Now we may state:

THEOREM 2.19. *For any* $\gamma \geqslant 50$

$$I(\gamma) < \gamma^2.$$

Proof. If G has $h+1$ primes we assume w.l.o.g. $v^2\gamma^3 > p_0 \cdots p_h > 2(h+1)^{h+1}$ (when $h \geqslant 16$). Then (2.14) with $\lambda = \frac{1}{2}$ gives $\iota < \gamma^2$ if

$$\gamma^{3/4} \geqslant v \cdot (g(h))^{3/2}.$$

Substituting for γ^3 the value $2(h+1)^{h+1}/v^2$ we get $2(h+1)^{h+1} \geqslant v^6 g^6(h)$. Taking for $v \leqslant \mu_G$ the trivial estimate $v < 3\log(h+1)$ we get finally

$$(h+1)^{h+1} \geqslant (729/2)(\log(h+1)\, g(h))^6.$$

Since the above inequality is always true if $h \geqslant 16$, we may restrict ourselves to consider groups with at most 16 primes.

Applying directly (2.14) with $h = 15$ and $\lambda = 1/2$ gives $\iota > \gamma^2$ provided

$$\gamma \geqslant v^{4/3} \prod_{i=1}^{15} \left(1 - \frac{1}{\sqrt{p_i}}\right)^{-2}.$$

We may assume $v \leqslant 5.5394$ since otherwise the asymptotic bound found above works, getting the bound $I(\gamma) < \gamma^2$ for γ greater than 100,000, say.

Now remark that by the condition (i) of Lemma 2.16, the restriction $v^2\gamma^2\eta > p_0 \cdots p_h$ can be strengthend to $v^2\gamma^3 D(\gamma, h) > p_0 \cdot \ldots \cdot p_h$, and we shall assume this.

If $\gamma < 100{,}000$, this gives $h \leqslant 12$ by looking at the exact values of $D(K, 13)$.

Now we apply the condition (ii) of Lemma 2.16 with the exact values of $D(K, h)$ given by the computer, obtaining the following table:

γ_0	γ_1	h	$v(\gamma_1)$	$D(\gamma_0,h)$	K	$D(K,h)$	$1/v$
1001	100,000	12	5.21	0.262	2100	0.191	0.192
265	1,000	9	4.375	0.339	781	0.214	0.228
106	264	7	3.75	0.391	266	0.266	0.267
75	105	6	3.75	0.395	186	0.265	0.267

(2.15)

where: γ is intended to run between γ_0 and γ_1; $h + 1$ is the largest number of primes allowed in the range $\gamma_0 \leqslant \gamma \leqslant \gamma_1$; K is chosen in order to verify the condition (ii) of Lemma 2.16.

Finally we can go down to $\gamma = 50$ by the following remark: Suppose $50 \leqslant \gamma \leqslant 74$ and put $\iota = x\eta$; if $x \geqslant 186$ then $\eta < \gamma D(186, 6) < \gamma/v$ and we are done. If $x < 186$, then $\iota < \gamma x D(x, 6) < \gamma \cdot 186 \cdot D(186, 6)$ since in the range $x \leqslant 186$ the function $x \cdot D(x, 6)$ attains its maximum at 186. Q.E.D.

Thus we have proved the bound (1.1) of Theorem 1 for any $\gamma \geqslant 50$. To deal with smaller values of γ we need more effective bounds of the number of primes essentially involved; this requests an other kind of considerations, which are developed in [1].

However all what we need to conclude the proof of (1.1) is the following remark, whose proof makes essential use of Lemmas 2.6, 2.8 and 2.10 of [1].

LEMMA 2.20. *Let G be a non-paracyclic group without cyclic normal Sylow subgroups.*

Then

(i) *if $\gamma_G \leqslant 20$ there are at most 4 primes dividing $|G|$;*

(ii) *if $\gamma_G \leqslant 50$ there are at most 5 primes dividing $|G|$.*

Proof. (i) By Lemma 2.6 no prime $\geqslant 7$ can divide η_G; moreover no pair of primes between 7 and 19 may fulfill the conditions of Lemma 2.8.

(ii) The above argument allows in case $\gamma_G \leqslant 50$ only one prime $\geqslant 13$ to divide η_G and only the following pairs of primes $\geqslant 7$ to divide $|G|$: (7, 29), (7, 43), (11, 23), (23, 47).

It is easily seen that only the triple 7, 11, 43 can be built up without violating Lemma 2.10: but then 5 cannot divide $|G|$ by the same lemma.

Q.E.D.

We now formalize the argument we used at the end of the proof of Theorem 2.19.

Remark 2.21. Assume $|G| = q_0^{a_0} \cdots q_h^{a_h}$. In order to ensure $\iota_G < \gamma_G^2$ it suffices to find K verifying

$$D(K, h) \leqslant 1/v_G \qquad \text{and} \qquad xD(x, h) \leqslant \gamma_G \qquad \forall\, x \leqslant K.$$

In fact, put $x = \iota_G/\eta_G$; if $x > K$, then (2.7) gives

$$\eta_G < \gamma_G \cdot D(K, h) \leqslant \gamma_G/v_G;$$

if $x \leqslant K$, then again (2.7) gives

$$\eta_G < \gamma_G \cdot D(x, h) \qquad \text{whence } \iota_G \leqslant \gamma_G x D(x, h) \leqslant \gamma_G^2.$$

Since in applying (2.7) Corollary 2.9 allows us to neglect cyclic normal Sylow subgroups, we may assume for h the strong bounds of Lemma 2.20.

Let us write down the following table:

γ_0	γ_1	v	h	K	$D(K, h)$	$KD(K, h)$
11	20	3	3	32	0.3225	10.32
21	50	3.75	4	76	0.2648	20.12

(2.16)

where, as in Table (2.15), $\gamma_0 \leqslant \gamma \leqslant \gamma_1$ is the range considered for $\gamma = \gamma_G$; v and h are the largest admissible values in the considered range of γ; K is chosen to maximize the function $xD(x, h)$ in the range $1 \leqslant x \leqslant K$.

It is apparent that the conditions of Remark 2.21 are fulfilled by the listed values of K, and Theorem 1 is now completely proved.

The lower bound of Theorem 2 for $I(\gamma)$ can be obtained from the following examples.

EXAMPLE 2.22. Let $p<q$ be prime numbers. Define the group $H^{(p,q)}=\langle a_1,\ldots,a_q,b\rangle$ by means of the relations

$$a_i^p=a_1\cdot a_2\cdots a_q=[a_i,a_j]=b^q=1$$
$$ba_ib^{-1}=a_{i+1}\qquad (i,j=1,\ldots,q(\mathrm{mod}\,q)).$$

All the elements of $H^{(p,q)}$ have order either p or q.

A direct computation yields

$$\iota_{H^{(p,q)}}=p^{q-1}\qquad\text{and}\qquad \gamma_{H^{(p,q)}}=p^{q-1}\left(1-\frac{1}{q}\right)+\frac{1}{q}.$$

EXAMPLE 2.23. Let $p<q$ be prime numbers and assume $p\mid q-1$ and $q<p^2$.

Define the group $K^{(p,q)}=\langle a_1,\ldots,a_q,b,c\rangle$ by means of the relations

$$a_i^p=b^p=c^q=[a_i,a_j]=a_1\cdot\ldots\cdot a_q=1$$
$$ca_ic^{-1}=a_{i+1},\ bcb^{-1}=c^r\ ba_ib^{-1}=a_{i\cdot r}\qquad (i,j=1,\ldots,q(\mathrm{mod}\,q))$$

with $r\neq 1$, $r^p\equiv 1(\mathrm{mod}\,q)$.

The orders of the elements of $K^{(p,q)}$ are p,p^2 and q.

A direct computation yields

$$\iota_{K^{(p,q)}}=p^{q-2}q\qquad\text{and}\qquad \gamma_{K^{(p,q)}}=p^{q-3}(pq-q+1).$$

To see that $I(\gamma)/\gamma$ is unbounded it suffices to take the direct product of suitable groups occurring in the above examples. Namely

EXAMPLE 2.24. Put

$$u_i=\begin{cases}p_{2i}\\ p_{2i+1}\end{cases}\qquad\text{and}\qquad v_i=\begin{cases}p_{2i+1} & i\leqslant 5\\ p_{2i+2} & i\geqslant 6\end{cases}$$

and

$$G_1=\mathfrak{A}_6\times K^{(7,43)}$$

$$G_{n+1}=G_n\times H^{(u_{n+1},v_{n+1})}.$$

Then

$$\iota_{G_n}=\iota_n=72\cdot 7^{41}\cdot 43\cdot\prod_{i=2}^{n}u_i^{v_i-1}$$

$$\gamma_{G_n}=\gamma_n=34\cdot 7^{40}\cdot 259\cdot\prod_{i=2}^{n}u_i^{v_i-1}\left(1-\frac{1}{v_i}+\frac{1}{v_iu_i^{v_i-1}}\right)$$
$$=\iota_n\frac{4403}{10836}\prod_{i=2}^{n}\left(1-\frac{1}{v_i}+\frac{1}{v_iu_i^{v_i-1}}\right).$$

Noting that for $i \geqslant 2$

$$\left(1-\frac{1}{p_i}+\frac{1}{p_i p_{i-1}^{p_i-1}}\right)^2 < \left(1-\frac{1}{p_i}\right)\left(1-\frac{1}{p_{i+1}}\right)$$

and using for $\prod_{i=1}^{n}(1-(1/p_i))$ the estimate (1.E), we get

$$\iota_n > \frac{10836}{4403}\gamma_n\left(\prod_{i=2}^{n}\left(1-\frac{1}{v_i}\right)\left(1-\frac{1}{u_i}\right)\right)^{-1/2}$$

$$> \frac{10836}{4403}\gamma_n \cdot \left(\frac{96e^c}{473}(\log(2n+4)+\operatorname{loglog}(2n+4))\right)^{1/2}.$$

Since obviously $\operatorname{loglog}\gamma_n < \log\frac{1}{2}p_{2n+3}^2 < 2(\log(2n+4)+\operatorname{loglog}(2n+4))$, we have an increasing sequence (γ_n, ι_n) verifying

$$\iota_n > \frac{10836}{4403}\gamma_n\left(\frac{48e^c}{473}\cdot\operatorname{loglog}\gamma_n\right)^{1/2} > \gamma_n(\operatorname{loglog}\gamma_n)^{1/2}. \tag{2.17}$$

Theorem 2 is then proved with $C_2 = 1$.

We conjecture, indeed, that the correct size of $I(\gamma)$ is essentially $\gamma\operatorname{loglog}\gamma$, and we sketch the argument we could use to obtain the lower bound

$$\limsup_{\gamma\to\infty}\frac{I(\gamma)}{\gamma\operatorname{loglog}\gamma} > \frac{1}{2}. \tag{2.18}$$

The arithmetical question of the existence, for any prime p_i, of a prime q_i verifying $q_i \equiv 1 (\operatorname{mod} p_i)$, $p_i^{3/2} < q_i < p_i^2$ is still unsolved, although there is a strong evidence for the positive answer.

Assuming this conjecture true, we can define a sequence of groups L_n built up like G_n by means of $K^{(p,q)}$ instead of $H^{(p,q)}$. Then we obtain a sequence

$$\gamma_n = 34 \cdot \prod_{i=3}^{n+1}{}^{*}\, p_i^{q_i-3}(p_i q_i - q_i + 1)$$

$$\iota_n = 72 \prod_{i=3}^{n+1}{}^{*}\, p_i^{q_i-2} q_i$$

where $*$ means that the ith factor is 1 if $p_i = q_j$ for some $j < i$.

A direct computation, using the estimate (1.E), gives

$$\iota_n/\gamma_n = \frac{72}{34}\prod_{i=3}^{n+1}{}^{*}\left(1-\frac{1}{p_i}+\frac{1}{p_i q_i}\right)^{-1} > \frac{1}{2}\operatorname{loglog}\gamma_n.$$

REFERENCES

1. R. DVORNICICH AND M. FORTI, Finite groups with few dth roots of 1, *J. Algebra* **91** (1984), 520–535.
2. R. DVORNICICH AND M. FORTI, "Paracyclic and Quasi-cyclic Groups," submitted for publication.
3. M. HAUSMAN AND H. N. SHAPIRO, On a family of almost cyclic finite groups, *Comm. Pure Appl. Math.* **33** (1980), 635–649.
4. B. HUPPERT, "Endliche Gruppen I," Springer-Verlag, Berlin, 1967.
5. J. B. ROSSER AND L. SCHOENFELD, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94.